Committee on National Security Systems

CNSS No. 24
May 2010

Policy

on

Assured Information Sharing (AIS) for

National Security Systems (NSS)

This document prescribes minimum standards.
Your department or agency may require further implementation.

CHAIR

FOREWORD

1. This document establishes the "Policy on Assured Information Sharing (AIS) for National Security Systems (NSS)." The United States Government is committed to responsibly sharing information through a risk-managed approach among authorized U.S. entities, pursuant to Executive Order 13526 (Reference A). Providing timely, secure information to decision makers, intelligence analysts, warfighters, and policy makers will enable efficient operations and protect the interests of the U.S. Government and American people. To complete this transition to a culture of AIS, individuals and organizations must establish a foundation to build trust by implementing common policies, practices, and processes. This effort will result in AIS within a trust-based environment in which information may be shared transparently and collaboratively, between authorized users.

2. This policy derives its authority from National Security Directive 42 (Reference B), which outlines the roles and responsibilities for securing NSS, and applicable sections of the Federal Information Security Management Act of 2002 (Reference C).

3. This policy also supports the *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, as well as national cybersecurity initiatives.

4. The Committee on National Security Systems (CNSS) Secretariat is tracking the status of the Member and Observer organizations' implementation of new and revised CNSS Issuances in order to create an Issuance Compliance Report. The Secretariat will oversee and administer this report process, which will be initiated six months following approval of this policy.

5. This policy is available from the CNSS Secretariat, as noted below, or the CNSS website: www.cnss.gov.

//s//
CHERYL J. ROBY

CNSS Secretariat (I923)
National Security Agency * 9800 Savage Road * Suite 6716 * Ft Meade MD 20755-6716
cnss@radium.ncsc.mil

POLICY ON ASSURED INFORMATION SHARING FOR NATIONAL SECURITY SYSTEMS

SECTION I—SCOPE

1. This document establishes the Policy on Assured Information Sharing (AIS) for National Security Systems (NSS). The document applies to Federal Government departments and agencies that own or operate NSS and any other entities that operate NSS on behalf of a Federal Government department or agency.

SECTION II—REFERENCES

2. Annex A lists referenced documents. Future updates to referenced documents shall be considered applicable to this policy.

SECTION III—DEFINITIONS

3. Definitions used in this policy are contained within Reference D, Annex B, or other references when specifically indicated.

SECTION IV—POLICY

4. Each Federal Government department and agency shall ensure the assured sharing of information by implementing the following measures:

a. General

(1) Develop and implement a policy-based decision-making process to oversee the assured sharing of information within and among security domains.

(2) Leverage existing information assurance (IA) policies, processes, and capabilities on networks and infrastructures, to the maximum extent possible.

(3) Optimize AIS among NSS, within given statutory and regulatory constraints, to protect information privacy guaranteed by Federal law and other legal rights of U.S. persons in accordance with Executive Order 13353, (Reference E).

b. Governance

(1) Establish a policy framework to enable information sharing among internal Committee on National Security Systems (CNSS) member and observer departments and agencies.

(2) Establish governance procedures to instill common processes, practices, and standards, and their compliance.

(3) Refer any issues regarding AIS to the CNSS governance structure.

c. Architecture

(1) Develop NSS Information Technology and IA architectures using the Federal Enterprise Architecture (FEA) and relevant National Institute of Standards and Technology standards.

(2) Ensure that departments and agencies reference the FEA Security and Privacy Profile (FEA SPP). (Reference F).

(3) Incorporate IA controls at the data, component, system, and service levels of NSS that manage risk and protect privacy, while allowing information to be shared across security domains.

(4) Integrate comprehensive IA capabilities (e.g., confidentiality, integrity, availability, non-repudiation, authorization, and authentication) into NSS to facilitate AIS.

(5) Include IA and AIS principles at the earliest possible point of the NSS system development life cycle to ensure the optimal approach for affecting engineering requirements and designing adequate information security into the program from the outset.

(6) Ensure AIS is addressed within existing department or agency-specific IA programs for NSS.

(7) Promote enhanced information sharing through discoverability, accessibility, and availability based on common tagging, retrieval, and dissemination standards applied across the NSS.

d. Information Assurance Risk Management

(1) Develop, establish, and implement an IA risk management program in accordance with CNSS Policy No. 22, (Reference G).

(2) Integrate lessons learned from exercises, risk assessments, and survivability assessments into requirements and procedures to advance AIS on NSS.

(3) Follow security-control assessment processes, procedures, and standards that support reciprocity throughout the Community of NSS users.

e. Technology

(1) In accordance with the Clinger-Cohen Act of 1996 (Reference H) and the National Security Telecommunications and Information Systems Security Policy No. 11, "National Information Assurance Acquisition Policy" (Reference I), use available commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) products, as first choice, when they are interoperable, cost effective, and meet IA and AIS requirements for NSS.

(2) Adhere to the existing CNSS security authorization process, CNSS Policy No. 6, (Reference J) , and the security categorization and control selection process, CNSS Instruction No. 1253 (Reference K), to implement IA controls in support of this policy selection.

(3) Identify and use, to the maximum extent applicable, Federal or industry best-practice AIS standards, technologies, and business processes that maximize the effectiveness of AIS. Use these applicable best practices to make NSS information available, as authorized, at all classification levels and across all infrastructures, whether virtual and/or under the direct control of the agency of origination that is providing and transferring the data.

f. Resources

(1) Plan, program, and budget for the appropriate resources to maintain and modernize AIS capabilities for NSS, in accordance with Office of Management and Budget (OMB) A-130, (Reference L).

(2) Ensure that all acquisitions related to NSS AIS capabilities incorporate IA life-cycle requirements and considerations throughout all phases, consistent with business needs and missions.

g. Culture

(1) Integrate an AIS training, education and awareness program for NSS into existing IA and security awareness training. Ensure that personnel are trained on an initial and recurring basis.

(2) Organizations should consider establishing incentives and other programs to encourage and reward AIS to enable a shift to a culture that supports the responsibility to share and provide, with authorized entities.

SECTION V—RESPONSIBILITIES

5. The CNSS will coordinate with the Director, OMB, to develop business standards for the FEA regarding AIS on NSS.

6. The heads of each Federal department or agency shall ensure the implementation of this policy and develop clear and comprehensive implementation guidance in support of current law, policies, regulations, and business rules

7. The CNSS will provide guidance to the Federal departments and agencies for using established AIS standards and best practices applicable to NSS.

SECTION VI—QUALIFICATIONS, EXCLUSIONS, AND EXCEPTIONS

8. This policy establishes a framework for supporting AIS among CNSS members. Based on threats and risk management, deliberations, and decisions, heads of Federal departments and agencies may impose, on their respective systems, more stringent IA measures, consistent with their responsibility to protect and to share.

Enclosures:
ANNEX A—References
ANNEX B—Definitions

ANNEX A

REFERENCES

a. Executive Order 13526, *Classified National Security Information,* December 29, 2009.

b. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

c. Public Law 107-347 [H.R. 2458], codified at 44 U.S.C. § 3541 et seq., *The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002*, December 17, 2002.

d. Committee on National Security Systems Instruction No. 4009, *National Information Assurance (IA) Glossary*, revised June 2006, or its successor.

e. Executive Order 13353, *Establishing the President's Board on Safeguarding Americans' Civil Liberties*, August 27, 2004.

f. *The Federal Enterprise Architecture Security and Privacy Profile,* Version 2.0, May 1, 2006.

g. Committee on National Security Systems Policy No. 22, *Information Assurance Risk Management Policy for National Security Systems*, February 2009.

h. Public Law 104–208 (PL 104-208), *Clinger-Cohen Act of 1996,* January 3, 1996.

i. National Security Telecommunications and Information Systems Security Policy No. 11: *National Information Assurance Acquisition Policy*, January 2000.

j. Committee on National Security Systems Policy No. 6 (CNSSP No. 6), *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems*, October 2005.

k. Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems,* October 2009.

l. Office of Management and Budget Transmittal Memorandum No. 4, Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

ANNEX B

DEFINITIONS

1. *Assured Information Sharing (AIS):* The ability to confidently share information with those who need it, when and where they need it, as determined by operational need and an acceptable level of security risk.

2. *Enterprise Architecture (EA):* A strategic information asset base that defines the mission, the information necessary for performing the mission, the technologies necessary for performing the mission, and the transitional processes for implementing new technologies in response to changing mission needs. The EA includes a baseline architecture, target architecture, and sequencing plan.

3. *Cross Domain Solution (CDS):* Information Assurance solution that provides the ability to access or transfer information between two or more domains.

4. *Federal Enterprise Architecture (FEA):* A business-based framework that the Office of Management and Budget (OMB) developed for government-wide improvement in developing EAs by providing a common framework to identify opportunities for simplifying processes and unifying work across the Federal Government.

5. *Information Assurance (IA):* Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

6. *National Security System (NSS)* (44 U.S.C. Section 3542(b)(2) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

7. *Security Domain:* A domain that implements a security policy and is administered by a single authority.